FAQ

FORTINET INTERNAL AND AUTHORIZED PARTNER USE ONLY

# Secure Wireless LAN (WLAN) Solution

## Frequently Asked Questions about Fortinet's Secure WLAN Solution

### What is Fortinet's Secure WLAN Solution?

The Fortinet Secure WLAN is a comprehensive, flexible solution that incorporates wireless and wired access, security, authentication, switching and management. The target market is distributerd enrerprises and small and mid-enterpise networks that need to adjust to the new demands for speed and security being put on their local area network as a result of the growth of mobile devices,

### What products make up Fortinet's Secure WLAN Solutions?

The core products in the Secure WLAN solution are the FortiGate, FortiWiFi, and FortiAP products. For larger, distributed organizations the FortiSwitch and FortiAuthenticator products offer specialized features that are also relevant.

### What new products are we launching?

For this launch we are announcing four new products. Two new FortiSwitch products and two new FortiAPs. All four products have different target audiences with the distributed enterprise

***FortiSwitch-28C, 348B*** – When deployed with FortiOS 5.0.2, the FortiSwitch-348B provides integration of Fortinet technologies. PoE functionality provides flexibility in deployment and eliminates the need to run additional wires to power wireless access points as well as FortiVoice IP phones, FortiCam IP surveillance cameras, and other devices such as retail PoS devices. The FortiSwitch-28C is ideal for small remote offices requiring switching functionality for FortiGate devices and networked PCs and printers.

***FortiAP-14C, 28C*** – Small, plug-and-play wireless remote access points allow organizations to easily and securely extend wireless access to small offices and telecommuters while retaining centralized policy control.

### How do we differentiate compared to the competition?

The Fortinet solutions combines comprehensive security and wireless access – providing authentication, authorization and policy enforcement in an easily managed system that allows system-wide policy enforcement. Security competitors such as Cisco, Checkpoint and Palo Alto Networks and wireless competitors such as Aruba and Aerohive cannot deliver this comprehensive solution

- Security companies such as Checkpoint and Palo Alto don't have wireless products
- Wireless companies such as Aruba and Aerohive have incomplete security

- Network companies such as Cisco and Juniper don't offer a unified, secure wireless solution.

**What is the target market for the Fortinet Secure WLAN Solution?**

Fortinet's Secure WLAN solution is appropriate for the distributed enterprise environment. This will be the target of our initial efforts.

**What pain points does the Fortinet Secure WLAN solution address?**

There are four key customer pain points that the Fortinet Secure WLAN addresses:

- The number of devices needing to connect to the network is increasing dramatically with the growth of smartphones and tablets. The nature of network traffic is shifting from wired to wireless. The Access points need to efficiently divide the available bandwidth among the users and applications based on priority. Security devices need to handle small packets with minimal latency, high connections per second and no per-user licensing. Users need to be authenticated with single sign on. And all the components need to operate and be managed as a secure, unified whole.
- Wireless troubleshooting is difficult, especially if there is an attack or worm outbreak, you can no longer pull a cable to isolate the offending user. More sophisticated detection algorithms are needed and APs need to be designed with security in mind, and not just access
- Cost of setup and operation of a network needs to be minimized. The days of per AP and per feature licenses which can drive up the cost are over. And the days of paying extra for a controller are over too.
- PCI Compliance for environments where critical customer information is being transported wirelessly, for example retail stores.

**Is this solution tied to a specific software release?**

Not necessarily. The new hardware can run on FortiGate devices running FortiOS v 5 However, to take advantage of all the latest features, FortiOS 5.0.2 is required. Some features that might be lacking from a previous release include:

- Wireless Controller in all FortiGates for consistent policy enforcement of all network traffic, both wired and wireless
- Bandwidth management built into the wireless solution allows organizations to prioritize mission-critical and bandwidth intensive applications.
- Device (including mobile devices/smartphones/tablets) and identity based policies
- Application Control
- Single-pane-of-glass management from FortiGate or globally from FortiManager
- Rogue AP detection and Wireless IPS
- Single profile change on FortiGate can propagate to 1000's of APs

**Are there vertical specific deployment examples you can provide?**

*Retail* – the 'store of the future' needs to leverage wireless technologies to better monetize the retail experience (e.g., 3rd party kiosks, location-specific offers sent directly to customers' mobile devices). Employee access and infrastructure (such as Point of Sale devices and video cameras) needs to be part of the same security infrastructure. Such a store would use FortiAP and/or FortiWiFi devices along with a FortiGate and a FortiSwitch. PCI-DSS regulations will need to be met. Organizations with large numbers of locations can benefit greatly by the ability of FortiManager and FortiAnalyzer to handle

thousands of locations.

*Healthcare* – Hospitals and other healthcare locations need to provide wireless access for Doctors and other practitioners in a secure, cost effective manner while meeting HIPAA and PCI requirements for secure wireless access. FortiAPs and FortiGate devices can meet the high-speed, low latency demands of such environments.

*Education* – K-12 and Higher Ed are dealing with the influx of smartphone and tablets into their networks. Per user and per access point licensing can very expensive for these organizations as the number of wireless users explodes. Network administrators need to apply very granular security policies while meeting regulatory requirements and preventing access to malicious, inappropriate, on file-sharing websites. These price sensitive customers can benefit greatly by the price/performance offered by our solution. Educational institutions are required to comply with CIPA and FERPA regulations. Fortinet management of the security policy and wireless provide an integrated platform for this reporting.